AN - 1995-120778 [16]
AP - JP19930203747 19930727
PR - JP19930203747 19930727
TI - Coding system for facsimile - generates common key for group of subscribers and encoding and decoding is done using this key
IW - CODE SYSTEM FACSIMILE GENERATE COMMON KEY GROUP SUBSCRIBER ENCODE DECODE KEY
PA - (CSKC-N) CSK CORP
PN - JP7046234 A 19950214 DW199516 H04L9/06 009pp
ORD - 1995-02-14
IC - G09C1/00 ; H04L9/06 ; H04L9/14
FS - GMPI;EPI
DC - P85 W01 W02
AB - J07046234 The coding system allocates unique ID for each and every subscriber in the list. A key generation centre (1) generates a secret key for every user. The key is selected by searching a hash table, that has the index ID of the subscriber in relation to a prime number. Each and every user is provided with the complete subscriber ID list, as open information.
- Multiple users of some group, like conference members, communicate from a single user, in the same way by the system. As the system generates a common key for the group, that requires only the information of IDs of the members then the ID and secret key is transmitted. The data is encrypted by the use of the common key and transmitted. The data is decrypted at the receiver's end by the use of the common key. Thus, group of users communicate from a single user by this method.
- ADVANTAGE - Uses common key for group of members. Uses simple algorithm for encryption/decryption. Enables maintenance of security. Facilitates easy processing.
- (Dwg.1/4)

3/3 (1/1 PAJ) - (C) PAJ / JPO
PN - JP7046234 A 19950214
AP - JP19930203747 19930727
PA - CSK CORP
IN - TANAKA HATSUICHI
I - H04L9/06 ; H04L9/14 ; G09C1/00
TI - CIPHERING SYSTEM
AB - PURPOSE:To realize sophisticated security with a simple algorithm by providing a reception terminal equipment generating a secret key through specific arithmetic operation, generating a common key between a key generating center and a conference member and decoding the received ciphering text with other common key generated by the common key or the like.
- CONSTITUTION:A key generating center 1 applies unidirectional Hash

functions f(), h() to each user 2 or the like based on the ID information intrinsic to user. Then a list of secret information sets P, Q, L, alpha, beta, gamma, delta, S and a public information N, subscriber ID list including a secret key G are generated by the arithmetic operation including an exponential function of a primitive element (g) of a prime. Thus, a common key is generated between the center 1 and conference membership without need of preliminary communication and the data are sent through ciphering by the common key. The receiver side generates a common key with the conference membership based on the secret key G, the ID information and the public information without need of preliminary communication and the reception terminal equipment decodes the received ciphering text.

ABV - 199505

ABD - 19950630

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－46234

(43)公開日　平成７年(1995)２月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		8837－5Ｌ			
				Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数５　ＦＤ　（全９頁）

(21)出願番号　特願平5－203747

(22)出願日　平成５年(1993)７月27日

(71)出願人　000131201
株式会社シーエスケイ
東京都新宿区西新宿２丁目６番１号

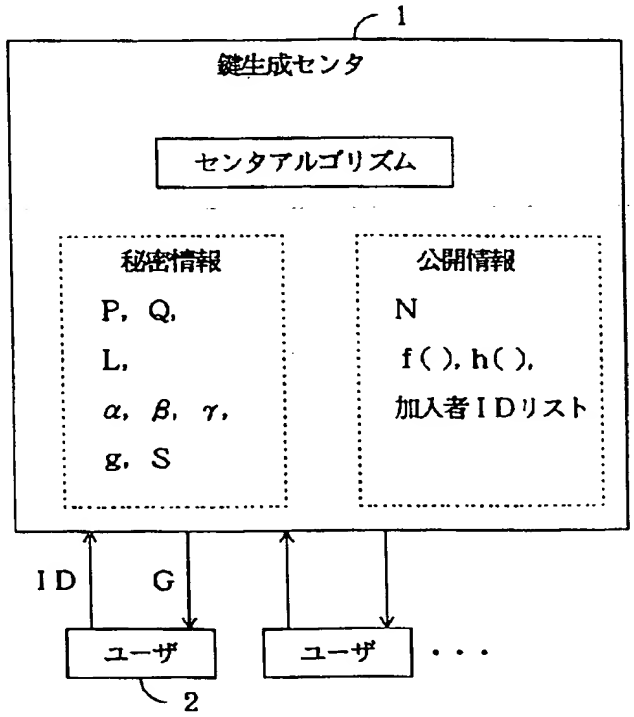
(72)発明者　田中　初一
兵庫県神戸市須磨区中落合４丁目２番467－302

(54)【発明の名称】　暗号システム

(57)【要約】　（修正有）

【目的】　シンプルなアルゴリズムでありながら高度のセキュリティを保ち、複数の者の間で暗号化・復号のための共通鍵を共有することができる暗号システムを提供する。

【構成】　通信に先立ち、鍵生成センタ１において、ユーザに対しその固有のＩＤ情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与する。加入者ＩＤリストを含む所定の情報は公開情報として各ユーザに提供する。送信側端末では送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他から予備通信を必要としないで共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する。受信側端末では受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他から予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する。



1

【特許請求の範囲】

【請求項１】　個々のユーザに対しそのユーザ固有のＩＤ情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与すると共に、各ユーザの加入者ＩＤリストを含む所定の情報を公開情報として提供する鍵生成センタと、

送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開情報とから送受信者間で予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する送信側端末と、

受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開情報とから送受信者間で予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する受信側端末とを備えたことを特徴とする暗号システム。

【請求項２】　鍵生成センタでは、

任意に選んだ２つの大きな素数Ｐ，Ｑに対して、

$N=PQ$

を計算してＮを公開情報にし、

$L=LCM\{P-1, Q-1\}=2\alpha\beta\gamma$　（LCM｛　｝＊

$K_M=(g_{Af}^{**}(\Pi_{m;M-A}\ I_{mf}))\cdot(g_{Ah}^{**}(\Pi_{m;M-A}\ I_{mh}))$　(mod N)

（$\Pi_{m;M-A}\ I_{mf}$は会議メンバーＭから送信側ユーザＡを除いた他のメンバーｍの全てにつきI_{mf}をかけ合わせることを意味）により共通鍵K_Mを計算し、

受信側端末では、

※

$K_M=(g_{Bf}^{**}(\Pi_{m;M-B}\ I_{mf}))\cdot(g_{Bh}^{**}(\Pi_{m;M-B}\ I_{mh}))$　(mod N)

（$\Pi_{m;M-B}\ I_{mf}$は会議メンバーＭから受信側ユーザＢを除いた他のメンバーｍの全てにつきI_{mf}をかけ合わせることを意味）により共通鍵K_Mを計算することを特徴とした請求項１記載の暗号システム。

【請求項３】　α，β，γを何らかの未知乱数でカバーして変形し、ＩＤ情報ID_mから２つの奇数I_{mf}，I_{mh}を何らかの手法により変形して得ることを特徴とした請求項２記載の暗号システム。

【請求項４】　鍵生成センタは生成した秘密の鍵をＩＣカードに記録して各ユーザに付与することを特徴とする請求項１、２または３記載の暗号システム。

【請求項５】　通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信することを特徴とする請求項１、２、３または４記載の暗号システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はメッセージ（電子情報）を安全に通信するための暗号システムに関するものであ★り、特に、ファックス等の郵便型暗号通信が可能で利用分野が広いと共に、複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵を用いることができるようにした暗号システムである。

2

＊は最小公倍数）

を満たすＬ，αおよび奇数β，γを求め、

Ｐ，Ｑの有限体ＧＦ（Ｐ），ＧＦ（Ｑ）の共通の原始元ｇを求め、

任意の一方向性ハッシュ関数ｆ（），ｈ（）を選択して公開情報にし、

ユーザｍのＩＤ情報であるID_mに対し、

$I_{mf}=2f(ID_m)+1$

$I_{mh}=2h(ID_m)+1$

を計算し、

$S_m=\beta I_{mf}+\gamma I_{mh}$　（mod Ｌ）　（modは法）

を計算して$g_{mf}=g^{**}(\alpha S_m\ \beta)$　(mod N)

$g_{mh}=g^{**}(\alpha S_m\ \gamma)$　(mod N)

（＊＊は左の値に対する右の値による冪乗）を計算し、

$G_m=\{g_{mf}, g_{mh}\}$

をユーザｍに会議用鍵生成のための秘密鍵として付与し、

送信側端末では、

送信側ユーザＡの秘密の鍵g_{Af}，g_{Ah}と他の会議メンバーのＩＤ情報ID_mおよび一方向性ハッシュ関数ｆ（），ｈ（）から

※受信側ユーザＢの秘密の鍵g_{Bf}，g_{Bh}と他の会議メンバーのＩＤ情報ID_mおよび一方向性ハッシュ関数ｆ（），ｈ（）から

【０００２】

【従来の技術】「電子情報」は本質的に物質やエネルギーと異なり、

①容易にコピーが可能である。

②オリジナルとコピーの区別がない。

③コピーされてもオリジナルに全くその痕跡を残さない。

という情報特有の性質があり、高度情報化社会の実現に大きく貢献すると共に、情報セキュリティの問題を発生する要因にもなるという「両刃の剣」を生み出している。

【０００３】かかる情報セキュリティを実現する手法として種々のものが提案されているが、従来より実用化されている暗号システムとしては、大別して次の２つの方式が存在する。

・共通鍵暗号系

3

・公開鍵暗号系

【0004】共通鍵暗号系とは、暗号化する鍵（暗号化鍵）と復号する鍵（復号鍵）とが同じものをいい、予めメッセージの送信側と受信側とで安全な手段により共通の鍵を受け渡しておき、送信側でその鍵により暗号化して送信されたものを受信側で同じ鍵で復号し、メッセージを受け取るものである。しかし、通信に先立って秘密を保った状態で鍵を引き渡す必要があるため、不便な点が多い。また、ユーザの数が多いと秘密に管理すべき鍵の数も非常に多くなり、管理が容易でないという不都合もある。

【0005】一方、公開鍵暗号系とは、ユーザ毎に暗号化鍵と復号鍵を一対ずつ作成し（任意に定めた復号鍵に対し、離散対数問題，ナップザック問題等で知られる一方向性関数により暗号化鍵を生成する。）、暗号化鍵を公開鍵リスト等で公開し、復号鍵のみを各ユーザにおいて秘密に保持しておき、送信側は受信側の公開された暗号化鍵でメッセージを暗号化して送信し、受信側では自己の復号鍵で復号を行ってメッセージを受け取るものである。なお、暗号化鍵を公開しても復号鍵が安全に保たれるのは、一方向性関数の性質に基づくものである。

【0006】この公開鍵暗号系では予め鍵を相手方と相互に持ち合う必要がないと共に、各ユーザは自己の鍵だけを持てばよいため、前述した共通鍵暗号系のような不都合はない。しかし、各ユーザの暗号化鍵を公開するための公開鍵リストを必要とすると共に、個々の公開鍵に認証機能を付与する必要があり、また、一般に公開鍵暗号系は暗号化および復号のアルゴリズムが複雑となってその演算を高速に行うのが技術的に困難であるという問題があった。

【0007】このような状況において「ＩＤ情報に基づく暗号系」が提案され、特にＩＤ情報から共通鍵を生成し、これにより暗号化・復号を行う場合には上記の公開鍵暗号系の不都合が解消されるため非常に有望である。

【0008】すなわち、ＩＤ情報に基づく暗号系では、信頼できる鍵生成センタの存在を前提とし、予め各ユーザ毎にＩＤ情報を登録すると共に、そのＩＤ情報に基づいて各ユーザに秘密の鍵を生成して付与し、各ユーザのＩＤ情報は公開する。そして、送信側のユーザは受信側のユーザの公開されたＩＤ情報およびその他の公開情報と自己の秘密の鍵とから共通鍵を生成し、これによりメッセージの暗号化を行って送信を行う。受信側のユーザは送信側のユーザの公開されたＩＤ情報およびその他の公開情報と自己の秘密の鍵とから共通鍵を生成し、これにより受信したメッセージの復号を行う。

【0009】従って、公開されるのはユーザの名前，住所，電話番号等に対応するＩＤ情報等であるため、公開鍵暗号系のように暗号化鍵を公開する方式に比べて便利かつ安全であると共に、暗号化，復号は共通鍵により行われるためアルゴリズムが簡素化できるものである。

4

【0010】

【発明が解決しようとする課題】このように、ＩＤ情報に基づく暗号系は非常に有効な方式であるとして種々の試みがなされているが、充分な安全性を持ったものがなく、特に複数（多数）のユーザによる結託によってセンタ秘密が解析され、任意のユーザ間の鍵が生成できてしまう等の欠点があった。

【0011】一方、本発明者は上記の欠点を解消した２者間の通信に適用できる暗号システムを既に開発し特許出願を行っているが、かかる出願においては複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵については考慮されていない。

【0012】本発明は上記の点に鑑み提案されたものであり、その目的とするところは、シンプルなアルゴリズムでありながら高度のセキュリティを保ち得ると共に、複数の者の間で暗号化・復号のための共通鍵を共有することができる会議用鍵を用いることができる暗号システムを提供することにある。

【0013】

【課題を解決するための手段】本発明は上記の目的を達成するため、個々のユーザに対しそのユーザ固有のＩＤ情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与すると共に、各ユーザの加入者ＩＤリストを含む所定の情報を公開情報として提供する鍵生成センタと、送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開情報とから送受信者間で予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する送信側端末と、受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開情報とから送受信者間で予備通信を必要としないで共通鍵を生成し、受信した暗号文を共通鍵により復号する受信側端末とを備えるようにしている。

【0014】また、共通鍵の秘匿性を高めるために通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信するようにすることもできる。

【0015】

【作用】本発明の暗号システムにあっては、通信に先立ち、鍵生成センタにおいて、個々のユーザに対しそのユーザ固有のＩＤ情報に基づいて一方向性ハッシュ関数の適用および素数の原始元を底とし法を用いた指数関数の適用を含む演算により秘密の鍵を生成してユーザ本人に付与する。また、各ユーザの加入者ＩＤリストを含む所定の情報は公開情報として各ユーザに提供する。

【0016】そして、メッセージの通信に際し、送信側端末では送信側ユーザの秘密の鍵と送信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開

5

情報とから予備通信を必要としないで会議メンバーとの間で共通鍵を生成し、この共通鍵によりメッセージを暗号化して送信する。また、受信側端末では受信側ユーザの秘密の鍵と受信側ユーザを除く会議メンバーの公開されたＩＤ情報およびその他の公開情報とから予備通信を必要としないで会議用共通鍵を生成し、受信した暗号文をその会議用共通鍵により復号する。

【００１７】一方、通信の開始時に作業鍵の情報を共通鍵により暗号化・復号して通信すると共に、その後は作業鍵によりメッセージを暗号化・復号して通信することにより、一層、共通鍵のセキュリティを高めることができる。

【００１８】

【実施例】以下、本発明の実施例につき図面を参照して＊説明する。

【００１９】図１は本発明の暗号システムにおける鍵生成センタの一実施例を示す構成図である。

【００２０】図１において、鍵生成センタ１は秘密情報と公開情報とを有し、新規に加入するユーザ２に対してそのユーザの名前，住所，電話番号等に応じたＩＤ情報ＩＤの登録を行うと共に、各情報に基づきセンタアルゴリズムにより秘密の鍵Ｇを付与する。なお、鍵Ｇは実際にはビットデータ列である。そのため、ＩＣカード等に記録して密かに付与するのが好ましい。

【００２１】以下、鍵生成センタ１における秘密情報，公開情報，センタアルゴリズムについて説明する。

【００２２】先ず、鍵生成センタ１では、任意に選んだ２つの大きな素数Ｐ，Ｑに対し、

$$N=PQ \tag{1}$$

を計算してＮを公開情報にする。

※　※【００２３】次いで、上記の素数Ｐ，Ｑに対し、

$$L=LCM\{P-1,\ Q-1\}=2\alpha\beta\gamma \tag{2}$$

を満たすＬ，αおよび奇数β，γを求める。ここで、ＬＣＭ｛Ｐ－１，Ｑ－１｝は（Ｐ－１）と（Ｑ－１）の最小公倍数を示している。

☆（），ｈ（）を選択し、これを公開情報にする。なお、一方向性ハッシュ関数としては、離散対数問題，ナップザック問題等で知られる関数が使用できる。

【００２４】次いで、素数Ｐ，Ｑの有限体ＧＦ（Ｐ），ＧＦ（Ｑ）の共通の原始元ｇを求める。

【００２６】次いで、ユーザｍのＩＤ情報であるＩＤ$_m$に対し、

【００２５】次いで、任意の一方向性ハッシュ関数ｆ　☆

$$I_{mf}=2f(ID_m)+1 \tag{3}$$

$$I_{mh}=2h(ID_m)+1 \tag{4}$$

を計算する。なお、各ユーザのＩＤ情報は加入者ＩＤリストによる公開情報とする。

☆【００２７】次いで、

☆

$$S_m=\beta I_{mf}+\gamma I_{mh} \pmod L \tag{5}$$

を計算する。なお、mod は法（ｍｏｄｕｌｕｓ）を示している。

◇【００２８】次いで、

◇

$$g_{mf}=g^{**}(\alpha S_m\ \beta) \pmod N \tag{6}$$

$$g_{mh}=g^{**}(\alpha S_m\ \gamma) \pmod N \tag{7}$$

を計算する。なお、「＊＊」は左の値に対する右の値による冪乗を示している。すなわち、ｇ＊＊（αS_m β）はｇの（αS_m β）乗を意味している。

＊【００２９】そして、上式で得られたg_{mf}，g_{mh}を組にした、

＊

$$G_m=\{g_{mf},\ g_{mh}\} \tag{8}$$

をユーザｍに会議用鍵生成のための秘密鍵としてＩＣカード等に記録して付与する。

※【００３３】また、送信側端末３には暗号化手段３１と共通鍵生成手段３２とが設けられ、受信側端末５，６，…には復号手段５１，６１，…と共通鍵生成手段５２，６２，…とが設けられている。

【００３０】なお、α，β，γを何らかの未知乱数でカバーして変形し、ＩＤ情報ＩＤ$_m$から２つの奇数I_{mf}，I_{mh}を何らかの手法により変形して得るようにすることもできる。

【００３４】以下、メッセージの送信および受信につき、各部の機能とともに、動作を説明する。なお、送信側端末３においてユーザＡが平文（暗号化されていない状態）のメッセージを受信側端末５のユーザＢに送信する場合を考える。

【００３１】次に、図２は会議メンバーに属する任意のユーザ間でメッセージの通信を行う際のシステム構成の例を示したものである。

【００３２】図２において、本システムは、ユーザＡが他の会議メンバーであるユーザＢ，Ｃ，…と暗号通信を行うための送信側端末３と、有線あるいは無線による通信路４と、ユーザＢ，Ｃ，…がメッセージの受信を行うための受信側端末５，６，…とから構成されている。

【００３５】先ず、送信側端末３の共通鍵生成手段３２においては、送信側ユーザＡの秘密の鍵g_{Af}，g_{Ah}と鍵生成センタ１の公開情報から得た他の会議メンバーのＩＤ情報ＩＤ$_m$および一方向性ハッシュ関数ｆ（），ｈ（）から

7

$$K_M = (g_{Af}{}^{**}(\Pi_{m;M-A}\ I_{mf})) \cdot (g_{Ah}{}^{**}(\Pi_{m;M-A}\ I_{mh})) \pmod N \quad (9)$$

により共通鍵K_Mを計算する。なお、$(\Pi_{m;M-A}\ I_{mf})$は会議メンバーMから送信側ユーザAを除いた他のメンバーmの全てにつきI_{mf}をかけ合わせることを意味している。

【００３６】そして、暗号化手段３１は算出された共通鍵K_Mによりメッセージを暗号化し、通信路４を介して＊受信側端末５に送信する。

【００３７】一方、受信側端末５の共通鍵生成手段５２においては、受信側ユーザBの秘密の鍵g_{Bf}，g_{Bh}と鍵生成センタ１の公開情報から得た他の会議メンバーのＩＤ情報I_{Dm}および一方向性ハッシュ関数ｆ（），ｈ（）から

8

$$K_M = (g_{Bf}{}^{**}(\Pi_{m;M-B}\ I_{mf})) \cdot (g_{Bh}{}^{**}(\Pi_{m;M-B}\ I_{mh})) \pmod N \quad (10)$$

により共通鍵K_Mを計算する。なお、$(\Pi_{m;M-B}\ I_{mf})$は会議メンバーMから受信側ユーザBを除いた他のメンバーmの全てにつきI_{mf}をかけ合わせることを意味している。

【００３８】そして、復号手段５１は算出された共通鍵K_Mにより通信路４を介して受信した暗号文を復号し、※平文のメッセージを得る。

【００３９】なお、式(9)，(10)により求めた共通鍵K_Mが互いに等しいことは次のようにして証明できる。

【００４０】式(9)は式(6)，(7)をg_{Af}，g_{Ah}に適用し、更に式(5)を適用すると、

$$\begin{aligned}K_M &= (g^{**}(\alpha S_A\ \beta\Pi_{m;M-A}\ I_{mf})) \cdot (g^{**}(\alpha S_A\ \gamma\Pi_{m;M-A}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha S_A\ (\beta\Pi_{m;M-A}\ I_{mf}+\gamma\Pi_{m;M-A}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha(\beta I_{Af}+\gamma I_{Ah})(\beta\Pi_{m;M-A}\ I_{mf}+\gamma\Pi_{m;M-A}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha\beta^2 I_{Af}\Pi_{m;M-A}\ I_{mf} + \alpha\beta\gamma(I_{Af}\Pi_{m;M-A}\ I_{mh}+I_{Ah}\Pi_{m;M-A}\ I_{mf}) + \alpha\gamma^2 I_{Ah}\Pi_{m;M-A}\ I_{mh}) \pmod N\end{aligned}$$

となる。ここで、

$2\alpha\beta\gamma = L = 0 \pmod L$

であり、$(I_{Af}\Pi_{m;M-A}\ I_{mh})$，$(I_{Ah}\Pi_{m;M-A}\ I_{mf})$はそれぞれ奇数となり、両者を加えたものは偶数となるため、K_Mを変形してきた最後の式の中間項は０となる。また、

$$K_M = g^{**}(\alpha(\beta^2\ \Pi_{m;M}\ I_{mf}+\gamma^2\ \Pi_{m;M}\ I_{mh})) \pmod N$$

となる。

【００４１】一方、式(10)は式(6)，(7)をg_{Bf}，g_{Bh}に適用し、これに式(5)を適用し、更に

$$\begin{aligned}K_M &= (g^{**}(\alpha S_B\ \beta\Pi_{m;M-B}\ I_{mf})) \cdot (g^{**}(\alpha S_B\ \gamma\Pi_{m;M-B}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha S_B\ (\beta\Pi_{m;M-B}\ I_{mf}+\gamma\Pi_{m;M-B}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha(\beta I_{Bf}+\gamma I_{Bh})(\beta\Pi_{m;M-B}\ I_{mf}+\gamma\Pi_{m;M-B}\ I_{mh})) \pmod N\\ &= g^{**}(\alpha\beta^2 I_{Bf}\Pi_{m;M-B}\ I_{mf} + \alpha\beta\gamma(I_{Bf}\Pi_{m;M-B}\ I_{mh}+I_{Bh}\Pi_{m;M-B}\ I_{mf}) + \alpha\gamma^2 I_{Bh}\Pi_{m;M-B}\ I_{mh}) \pmod N\\ &= g^{**}(\alpha(\beta^2\ \Pi_{m;M}\ I_{mf}+\gamma^2\ \Pi_{m;M}\ I_{mh})) \pmod N\end{aligned}$$

となり、両式は一致する。従って、K_Mを共通鍵暗号系の鍵として暗号化・復号することによりメッセージの暗号通信を行うことができる。

【００４２】一方、本システムのセキュリティがどうして高いかを示す必要があるが、暗号システムが絶対に安全であるということは理論的には証明できない。すなわち、アタック（暗号解析）が可能であることが証明されないことが、安全性の証明になる。ただし、定性的にセキュリティの高さの根拠を示せば次のようになる。

【００４３】①式(1)においてＮは公開情報であるが、このＮから素数Ｐ，Ｑを算出することは計算量的に不可能である。

【００４４】②式(2)により生成される秘密情報Ｌ，α，β，γは素数Ｐ，Ｑからそれぞれ１を引いたものの

★　$I_{Af}\Pi_{m;M-A}\ I_{mf} = \Pi_{m;M}\ I_{mf}$
　　$I_{Ah}\Pi_{m;M-A}\ I_{mh} = \Pi_{m;M}\ I_{mh}$
となる。なお、$(\Pi_{m;M}\ I_{mf})$は会議メンバーMのメンバーmの全てにつきI_{mf}をかけ合わせることを意味している。$(\Pi_{m;M}\ I_{mh})$についても同様である。よって、

★30

☆　$2\alpha\beta\gamma = L = 0 \pmod L$
を適用すると、

☆

最小公倍数およびその素因数であるため、Ｎの素因数分解が分からない限り公開情報から割り出すことは殆ど不可能であり、これらを各所の式に用いているため、値の不規則性が高く、種々の数学的手法による解析が適用しにくい。

【００４５】❸素数Ｐ，Ｑの有限体ＧＦ（Ｐ），ＧＦ（Ｑ）の共通の原始元ｇはそれ自体が公開情報から割り出されることは殆ど不可能であり、これを式の途中に用いているため、値の不規則性が高く、種々の数学的手法による解析が適用しにくい。

【００４６】❹式(3)，(4) において一方向性ハッシュ関数ｆ（），ｈ（）を用いているため、逆方向の数学的解析は殆ど不可能である。

【００４７】❺式(6)，(7) において原始元ｇの冪乗（指数）およびＮの法を用いているため、逆方向の数学的解析はほとんど不可能である。従って、ユーザが自己の秘密の情報を用い、あるいは複数のユーザが結託してそれぞれの秘密の情報を提供し合っても、センタ秘密を解析することは殆ど不可能である。

【００４８】次に、図３は本発明の他の実施例を示したものであり、より共通鍵ならびにメッセージのセキュリティを高めたものである。なお、鍵生成センタ１の構成および動作は前述したものと同様である。

【００４９】図３においては、図２の構成に比して、送信側端末３に作業鍵保持手段３３と鍵切換手段３４が付加され、受信側端末５，６，…にも作業鍵保持手段５３，…と鍵切換手段５４，…が付加されている。

【００５０】動作にあたり、送信側端末３においてユーザＡが平文（暗号化されていない状態）のメッセージを受信側端末５のユーザＢに送信する場合は次のようになる。

【００５１】先ず、送信側端末３の共通鍵生成手段３２においては、送信側ユーザＡの秘密の鍵g_{Af}，g_{Ah}と鍵生成センタ１の公開情報から得た他の会議メンバーのＩＤ情報ID_mおよび一方向性ハッシュ関数ｆ（），ｈ（）から共通鍵K_Mを計算する。

【００５２】これとほぼ同時に、作業鍵保持手段３３はユーザＡから与えられた任意の作業鍵K_Wを保持し、通信開始時のメッセージとして暗号化手段３１に与えると共に、鍵切換手段３４にも与える。

【００５３】鍵切換手段３４は通信の開始時の一定期間は共通鍵生成手段３２からの共通鍵K_Mを通過させて暗号化手段３１に与え、一定期間の経過後は作業鍵保持手段３３からの作業鍵K_Wを暗号化手段３１に与える。

【００５４】従って、暗号化手段３１は通信の開始時の一定期間は共通鍵K_Mを暗号化鍵として用い、作業鍵K_Wの情報をメッセージとして送信する。

【００５５】受信側端末５でも同様に共通鍵生成手段５２が共通鍵K_Mを生成し、鍵切換手段５４は通信の開始時においてはこの共通鍵K_Mを復号手段５１に与える。

【００５６】従って、通信路４を介して送信側端末３から送られてきた作業鍵K_Wの暗号化されたメッセージは共通鍵K_Mにより復号手段５１が復号し、これを作業鍵保持手段５３が保持する。

【００５７】そして、作業鍵K_Wの情報が受信側端末５に完全に伝わった後、両端末３，５の鍵切換手段３４，５４は暗号化手段３１に与える暗号化鍵を作業鍵K_Wに切り換え、その後は本来送信したいメッセージを作業鍵K_Wを用いて暗号化，復号して通信する。従って、暗号文は図４に示すような状態となる。なお、作業鍵K_Wは任意に設定できると共に、通信の途中で自由に変更することもできる。

【００５８】この実施例の場合、ユーザＡ，Ｂ，Ｃ，…を含む会議メンバーＭの間では一つしかない共通鍵K_Mを通信開始時の短時間しか使用せず、その後は任意の作業鍵K_Wを使って通信が行えるため、共通鍵ならびにメッセージのセキュリティをより一層向上させることができる。

【００５９】

【発明の効果】以上説明したように、本発明の暗号システムにあっては、ＩＤ情報に基づく暗号系を基本として、ファックスのような郵便型の暗号通信を可能にし、また、アタック（暗号破り）を防止するための種々の工夫を加えているため、シンプルなアルゴリズムでありながら高度のセキュリティを保ち得るという効果がある。更に、複数の者の間で共有できる会議用鍵を用いることができるため、同じ内容のメッセージを複数の者に送信する場合に送信が１回で済み、処理が容易になるという効果がある。

【図面の簡単な説明】

【図１】本発明の暗号システムにおける鍵生成センタの一実施例を示す構成図である。

【図２】本発明の暗号システムにおける送信側および受信側の端末の一実施例を示す構成図である。

【図３】本発明の暗号システムにおける送信側および受信側の端末の他の実施例を示す構成図である。

【図４】図３の実施例における暗号文の論理的構成を示す図である。

【符号の説明】

１……鍵生成センタ
２……ユーザ
３……送信側端末
３１…暗号化手段
３２…共通鍵生成手段
３３…作業鍵保持手段
３４…鍵切換手段
４……通信路
５……受信側端末
５１…復号手段

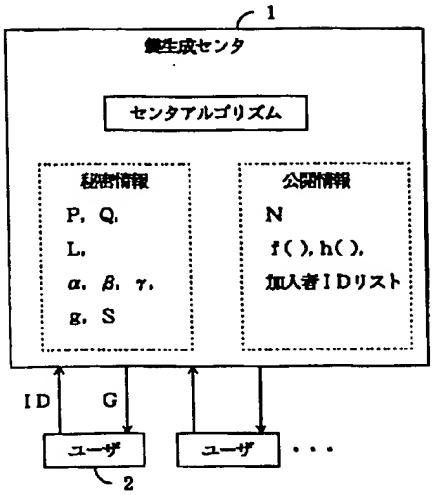
11

52…共通鍵生成手段
53…作業鍵保持手段
54…鍵切換手段

12

6……受信側端末
61…復号手段
62…共通鍵生成手段

【図1】

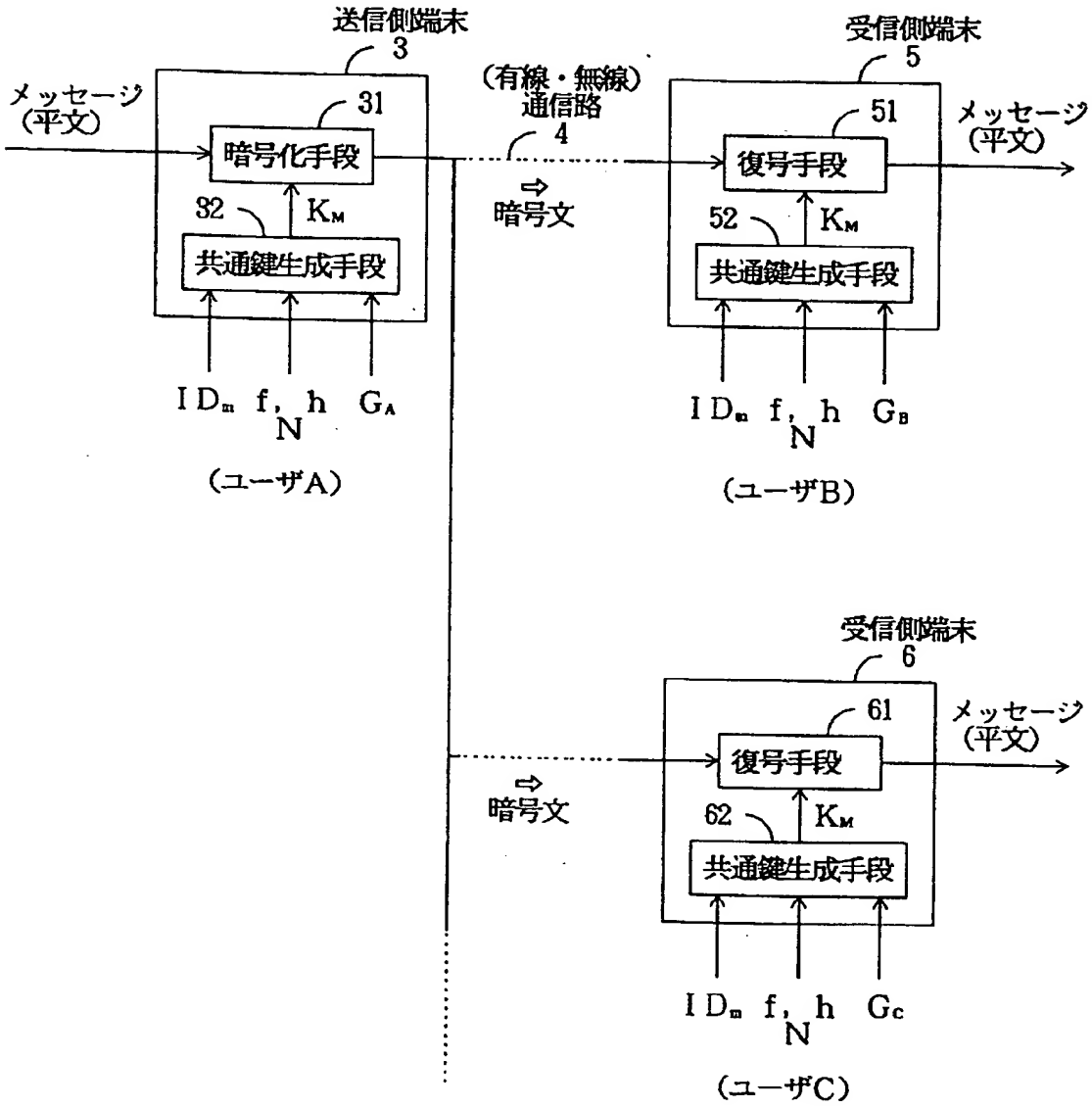


【図4】

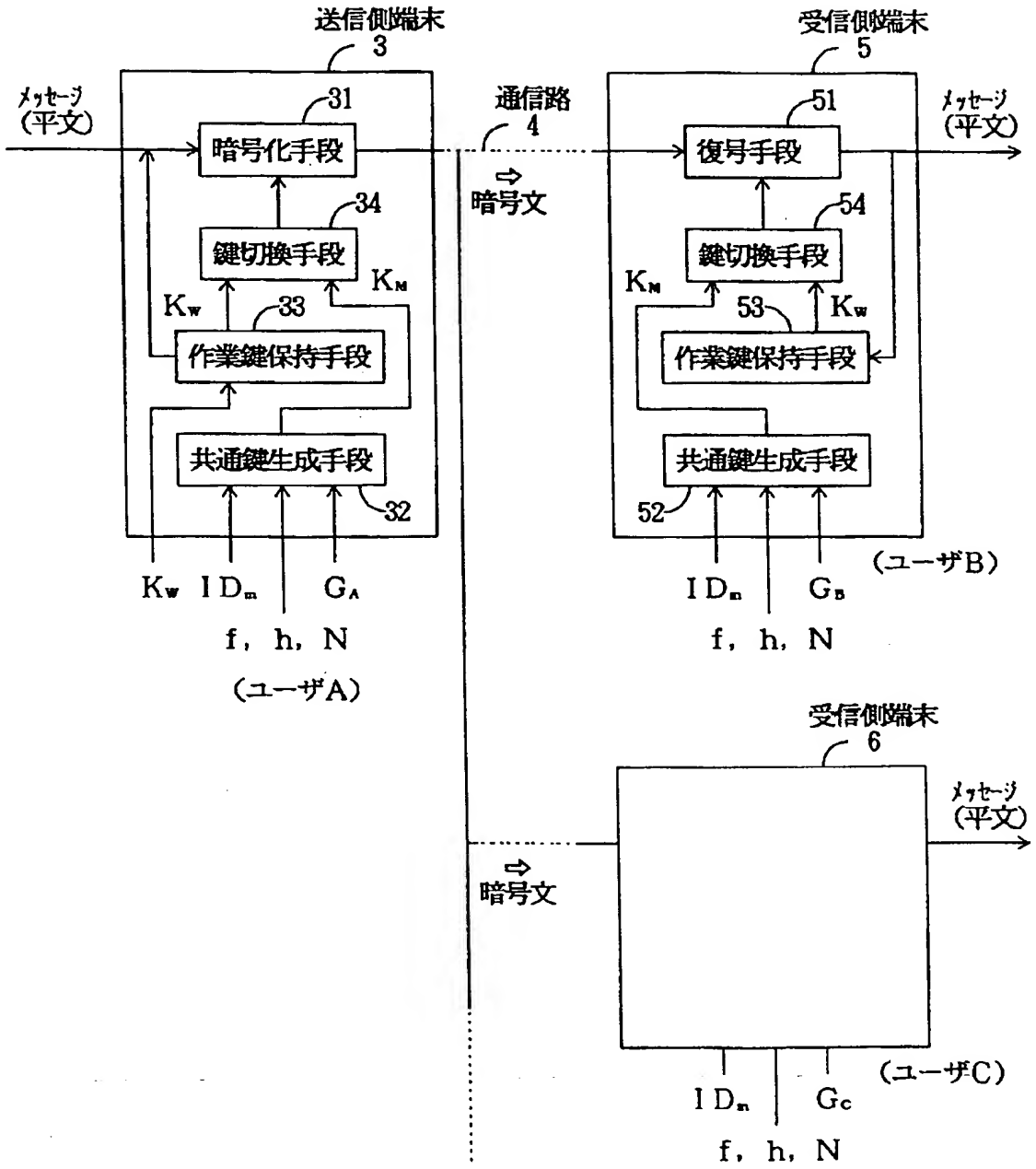
暗号文

K_W についての情報 (K_M で暗号化)	メッセージ (K_W で暗号化)

【図２】


送信側端末
3
メッセージ
(平文)
31
暗号化手段
32
K_M
共通鍵生成手段
ID_m f, h, N G_A
(ユーザA)
(有線・無線)
通信路
4
⇨
暗号文
受信側端末
5
51
復号手段
52
K_M
共通鍵生成手段
ID_m f, h, N G_B
(ユーザB)
メッセージ
(平文)
受信側端末
6
61
復号手段
62
K_M
共通鍵生成手段
ID_m f, h, N G_C
(ユーザC)
メッセージ
(平文)
⇨
暗号文

【図3】


送信側端末
3
受信側端末
5
受信側端末
6
メッセージ
(平文)
31
暗号化手段
通信路
4
暗号文
51
復号手段
メッセージ
(平文)
34
鍵切換手段
54
鍵切換手段
K_M
K_W
33
作業鍵保持手段
53
作業鍵保持手段
共通鍵生成手段
32
52
共通鍵生成手段
K_W ID_m G_A
f, h, N
(ユーザA)
ID_m G_B
f, h, N
(ユーザB)
暗号文
メッセージ
(平文)
ID_m G_C
f, h, N
(ユーザC)